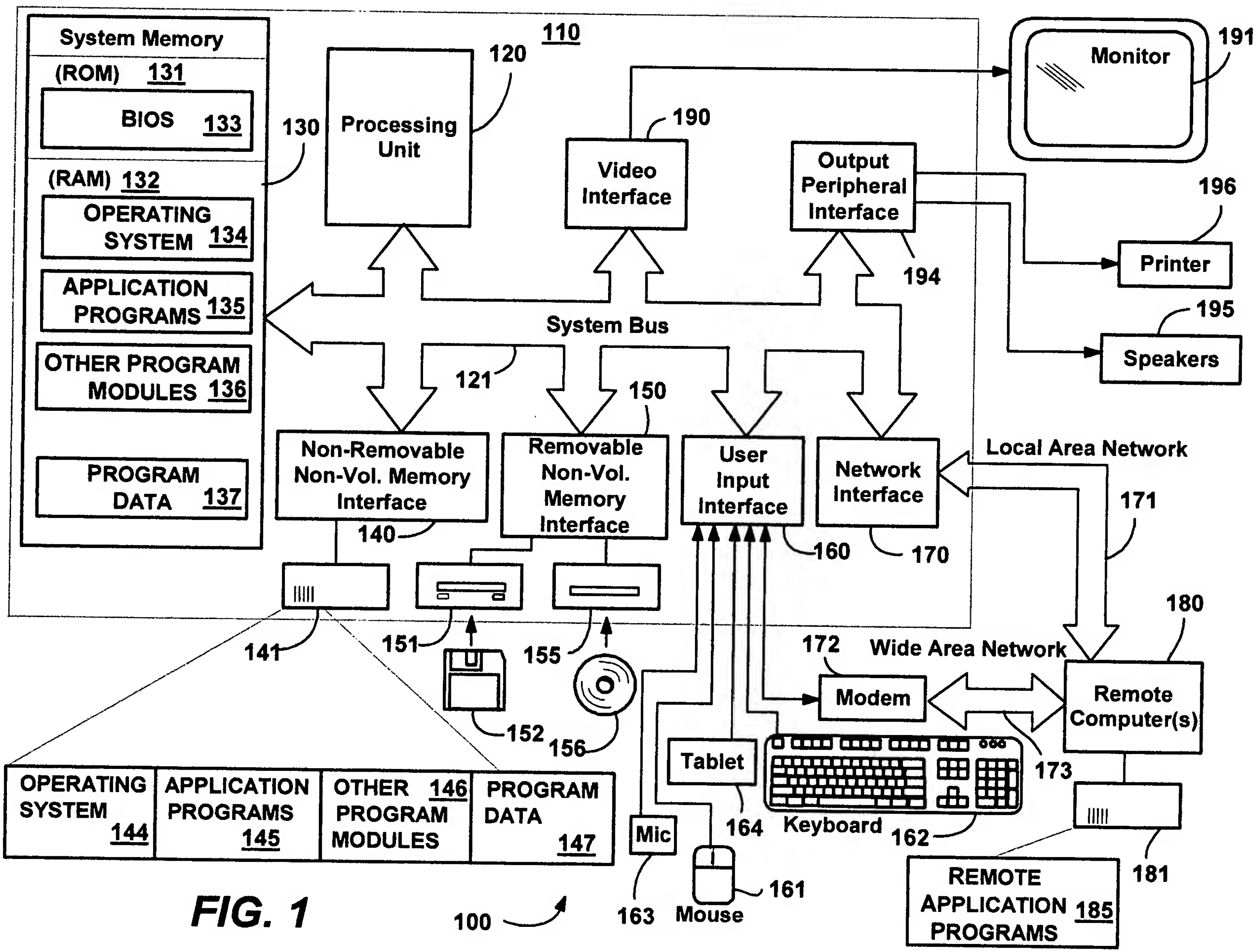


System Memory
(ROM) 131
BIOS 133
(RAM) 132
OPERATING SYSTEM 134
APPLICATION PROGRAMS 135
OTHER PROGRAM MODULES 136
PROGRAM DATA 137
130
Processing Unit
120
110
Video Interface
190
Output Peripheral Interface
194
Monitor
191
196
Printer
195
Speakers
System Bus
121
Non-Removable Non-Vol. Memory Interface
140
Removable Non-Vol. Memory Interface
150
User Input Interface
160
Network Interface
170
Local Area Network
171
180
Remote Computer(s)
Wide Area Network
172
Modem
173
141
151
155
152
156
OPERATING SYSTEM 144
APPLICATION PROGRAMS 145
OTHER PROGRAM MODULES 146
PROGRAM DATA 147
Tablet
164
Keyboard
162
Mic
163
Mouse
161
181
REMOTE APPLICATION PROGRAMS 185
100

FIG. 1

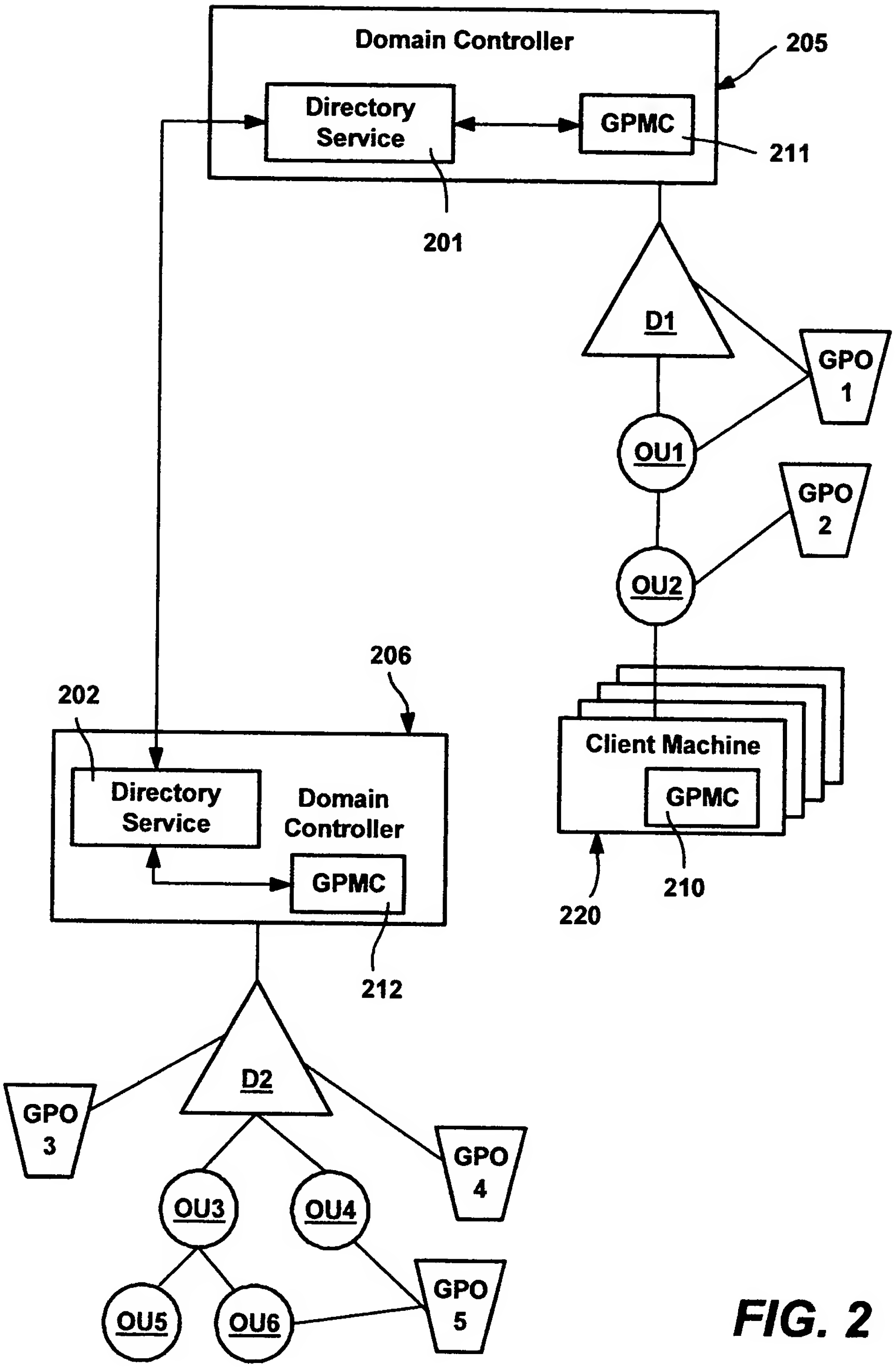

Domain Controller
205
Directory Service
GPMC
211
201
D1
GPO 1
OU1
GPO 2
OU2
206
202
Directory Service
Domain Controller
GPMC
212
Client Machine
GPMC
220
210
D2
GPO 3
GPO 4
OU3
OU4
GPO 5
OU5
OU6

FIG. 2

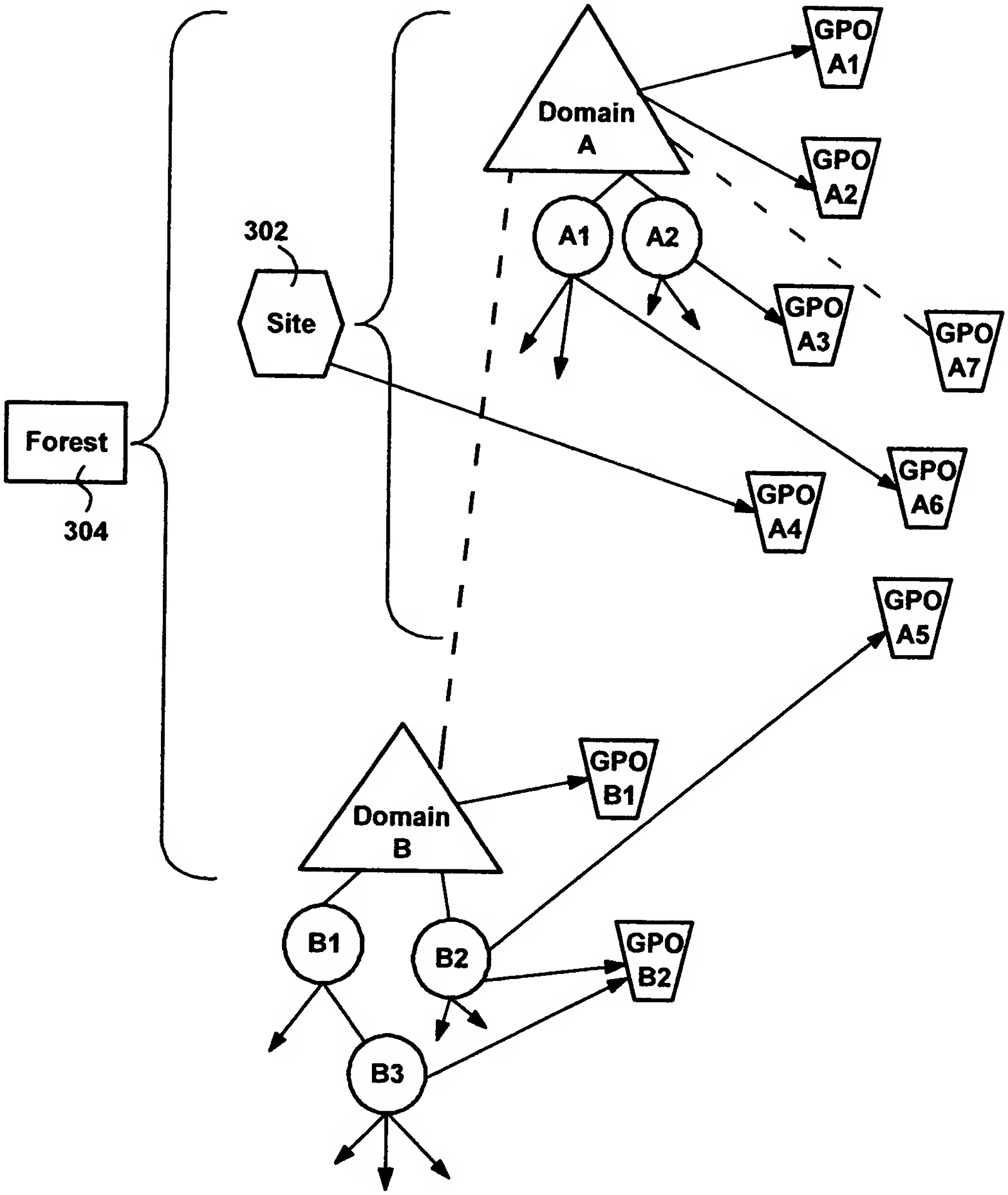

Forest
304
302
Site
Domain A
A1
A2
GPO A1
GPO A2
GPO A3
GPO A7
GPO A4
GPO A6
GPO A5
Domain B
GPO B1
B1
B2
B3
GPO B2

FIG. 3

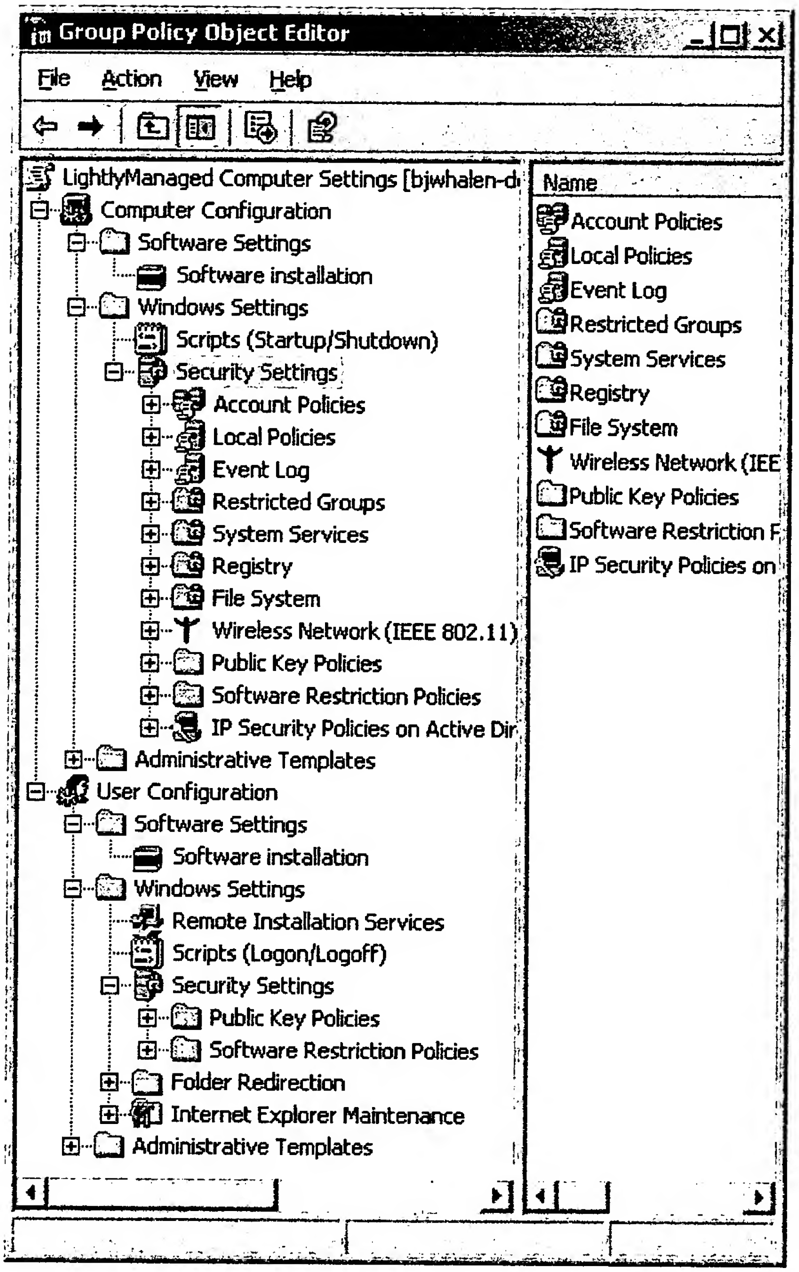
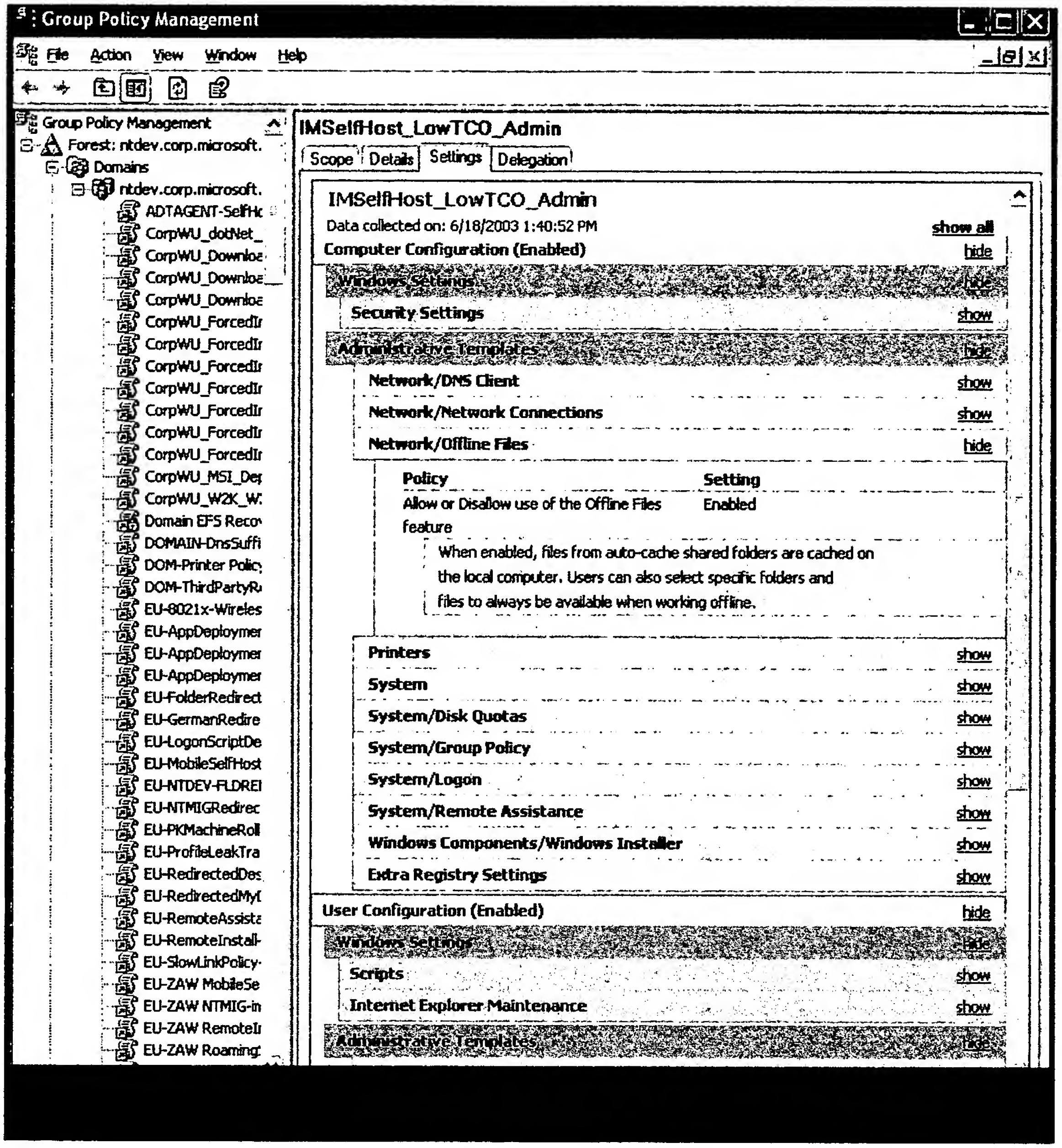


FIG. 4
Prior art



IMSelfHost_LowTCO_Admin

Data collected on: 6/18/2003 1:40:52 PM — show all

Computer Configuration (Enabled) — hide

Windows Settings — hide

Security Settings — show

Administrative Templates — hide

Network/DNS Client — show

Network/Network Connections — show

Network/Offline Files — hide

Policy	Setting
Allow or Disallow use of the Offline Files feature	Enabled

When enabled, files from auto-cache shared folders are cached on the local computer. Users can also select specific folders and files to always be available when working offline.

Printers — show

System — show

System/Disk Quotas — show

System/Group Policy — show

System/Logon — show

System/Remote Assistance — show

Windows Components/Windows Installer — show

Extra Registry Settings — show

User Configuration (Enabled) — hide

Windows Settings — hide

Scripts — show

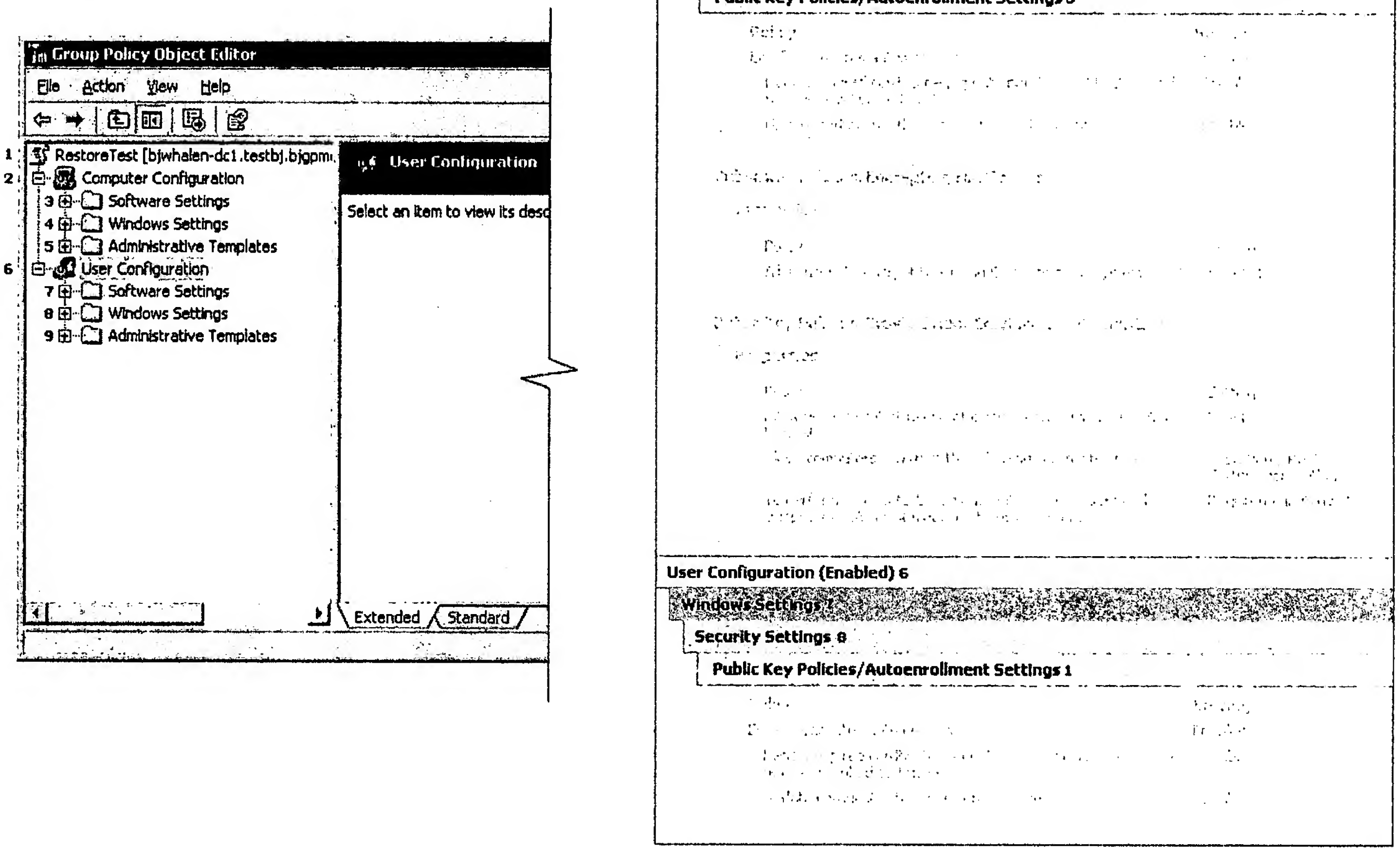
Internet Explorer Maintenance — show

Administrative Templates — hide

FIG. 5

Tree to Report Mapping

Highest Level (consistent) buckets



Group Policy Object Editor

1 RestoreTest [bjwhalen-dc1.testbj.bjgpm.

2 Computer Configuration

3 Software Settings

4 Windows Settings

5 Administrative Templates

6 User Configuration

7 Software Settings

8 Windows Settings

9 Administrative Templates

User Configuration

Select an item to view its desc

RestoreTest 1

Data collected on: 6/19/2003 1:19:27 PM

Computer Configuration (Enabled) 2

Windows Settings 3

Security Settings 4

Public Key Policies/Autoenrollment Settings 5

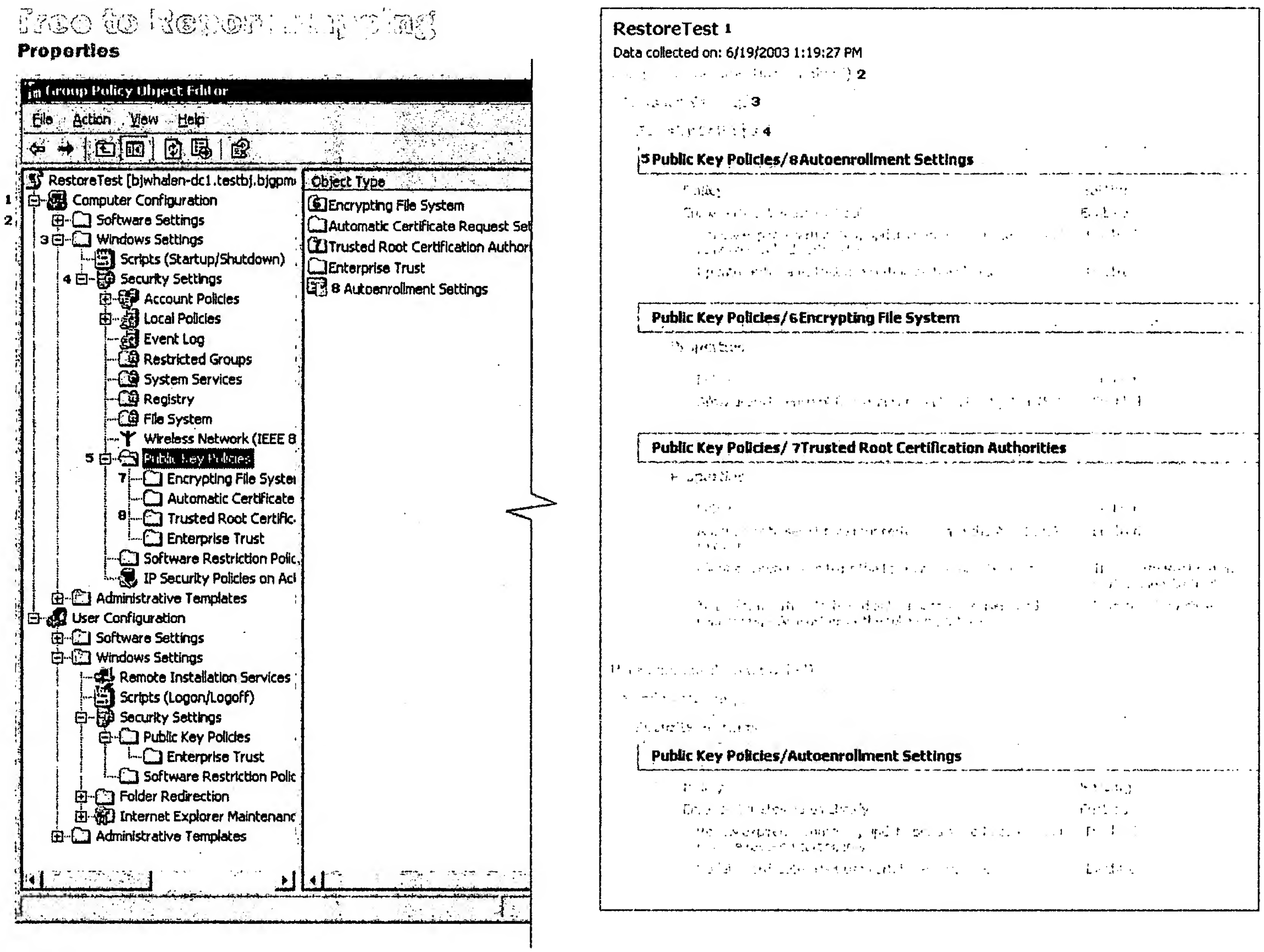
User Configuration (Enabled) 6

Windows Settings 7

Security Settings 8

Public Key Policies/Autoenrollment Settings 1

FIG. 6



RestoreTest 1

Data collected on: 6/19/2003 1:19:27 PM

2

3

4

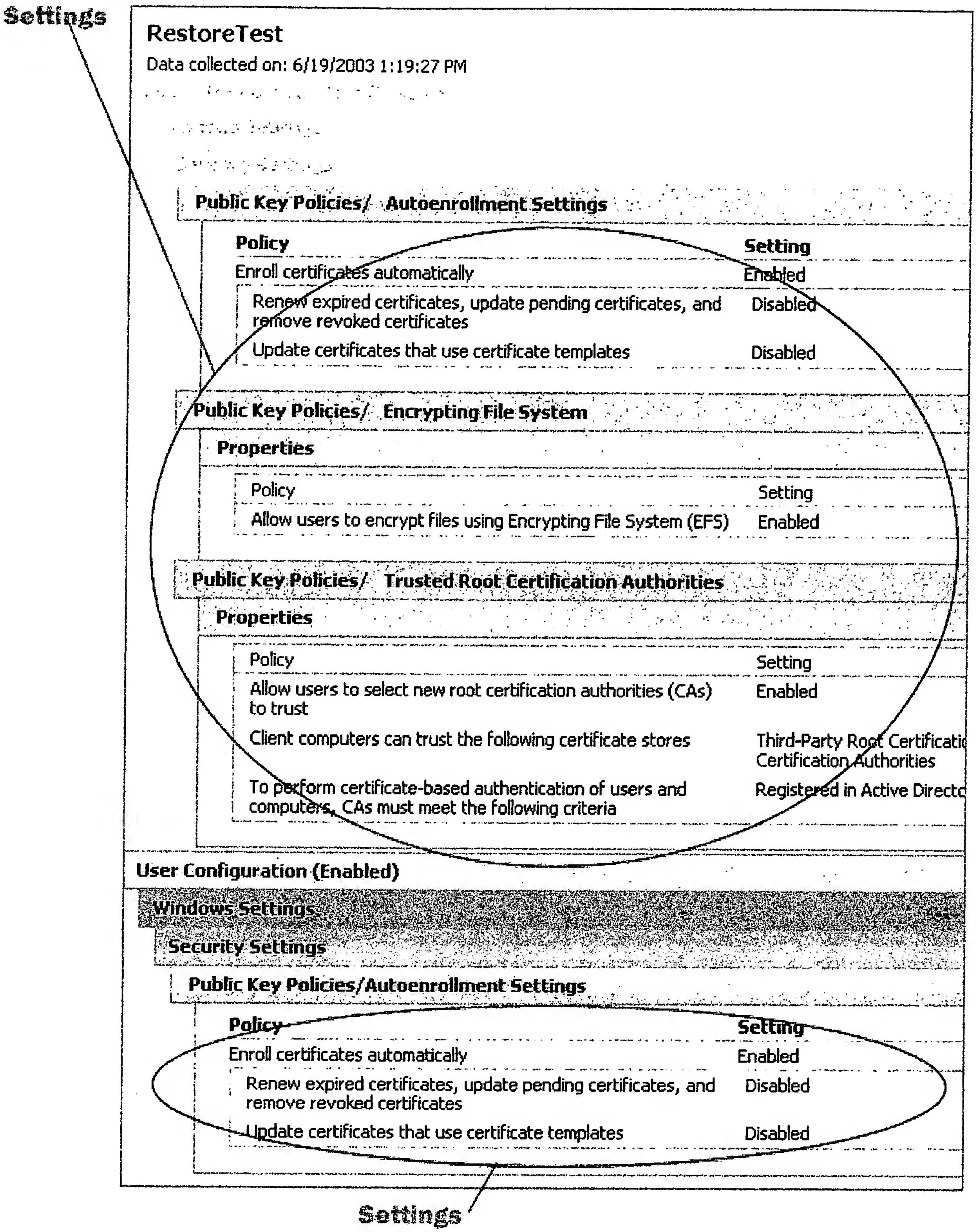
5 Public Key Policies/8 Autoenrollment Settings

Public Key Policies/6 Encrypting File System

Public Key Policies/ 7 Trusted Root Certification Authorities

Public Key Policies/Autoenrollment Settings

FIG. 7



RestoreTest

Data collected on: 6/19/2003 1:19:27 PM

[illegible]

[illegible]

[illegible]

Public Key Policies/ Autoenrollment Settings

Policy	**Setting**
Enroll certificates automatically	Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates	Disabled
Update certificates that use certificate templates	Disabled

Public Key Policies/ Encrypting File System

Properties

Policy	Setting
Allow users to encrypt files using Encrypting File System (EFS)	Enabled

Public Key Policies/ Trusted Root Certification Authorities

Properties

Policy	Setting
Allow users to select new root certification authorities (CAs) to trust	Enabled
Client computers can trust the following certificate stores	Third-Party Root Certificati Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directo

User Configuration (Enabled)

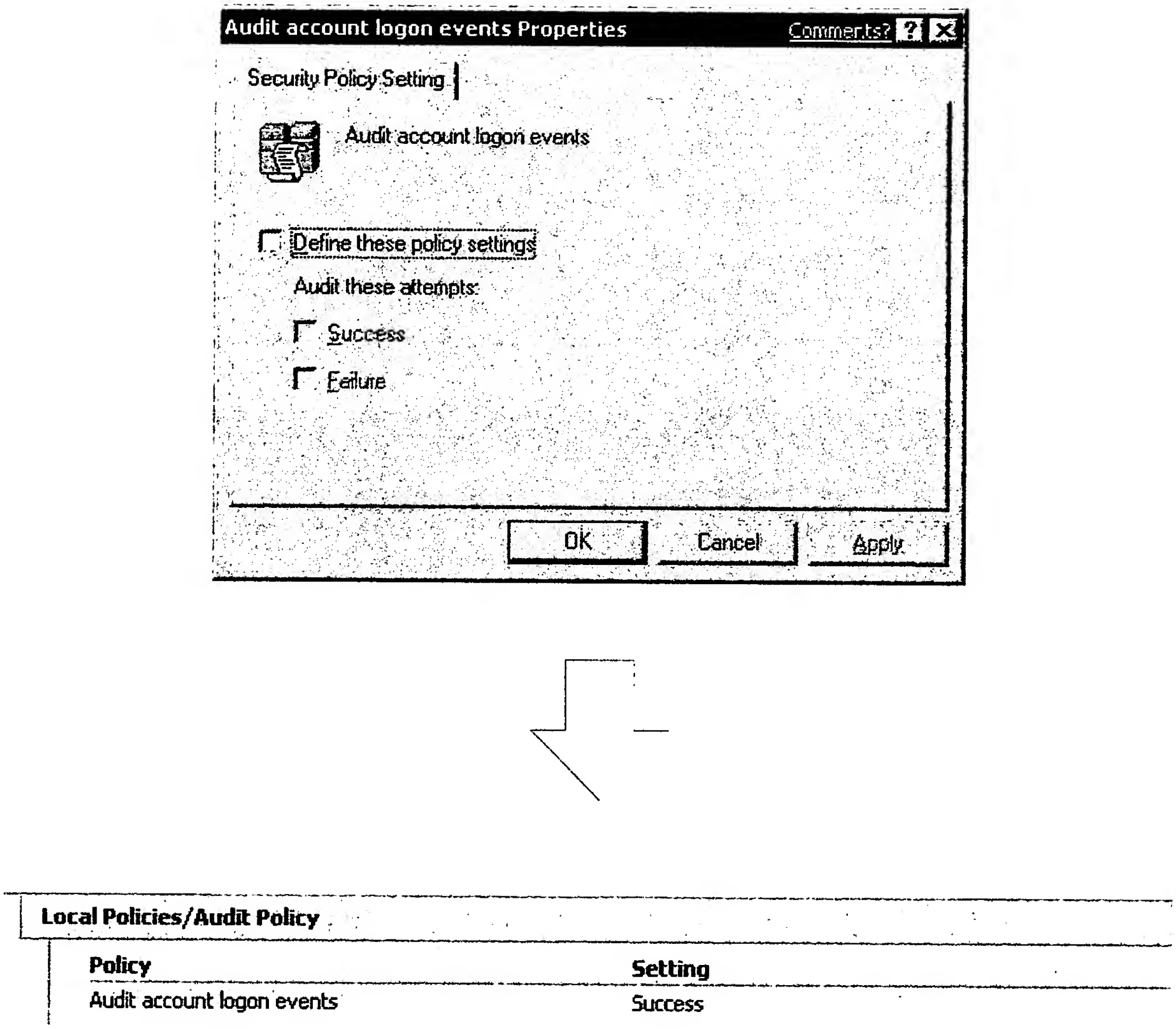
Windows Settings

Security Settings

Public Key Policies/Autoenrollment Settings

Policy	**Setting**
Enroll certificates automatically	Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates	Disabled
Update certificates that use certificate templates	Disabled

FIG. 8



Audit account logon events Properties

Security Policy Setting

Audit account logon events

□ Define these policy settings

Audit these attempts:

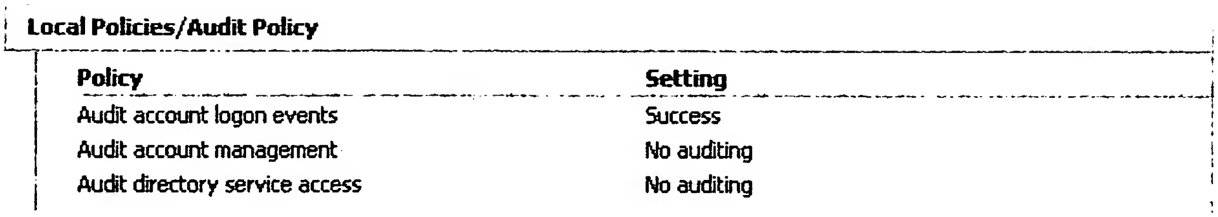
□ Success

□ Failure

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success

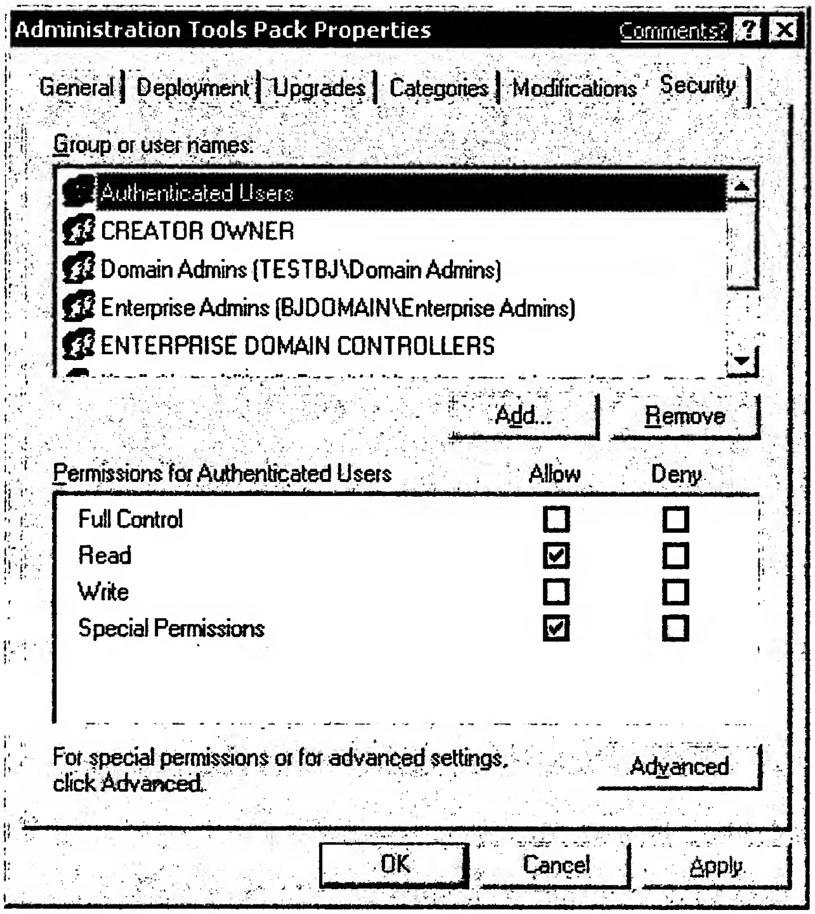
FIG. 9



Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success
Audit account management	No auditing
Audit directory service access	No auditing

FIG. 10



Administration Tools Pack Properties

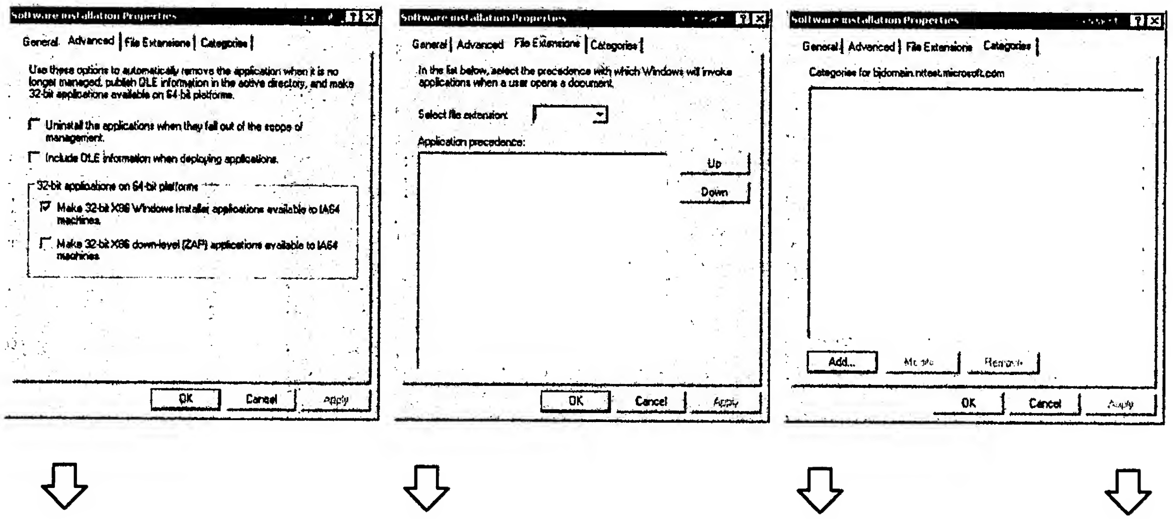
Group or user names:

- Authenticated Users
- CREATOR OWNER
- Domain Admins (TESTBJ\Domain Admins)
- Enterprise Admins (BJDOMAIN\Enterprise Admins)
- ENTERPRISE DOMAIN CONTROLLERS

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced.

FIG. 12
Prior Art



Use these options to automatically remove the application when it is no longer managed, publish OLE information in the active directory, and make 32-bit applications available on 64-bit platforms.

□ Uninstall the applications when they fall out of the scope of management.

□ Include OLE information when deploying applications.

32-bit applications on 64-bit platforms

☑ Make 32-bit X86 Windows Installer applications available to IA64 machines.

□ Make 32-bit X86 down-level (ZAP) applications available to IA64 machines.

In the list below, select the precedence with which Windows will invoke applications when a user opens a document.

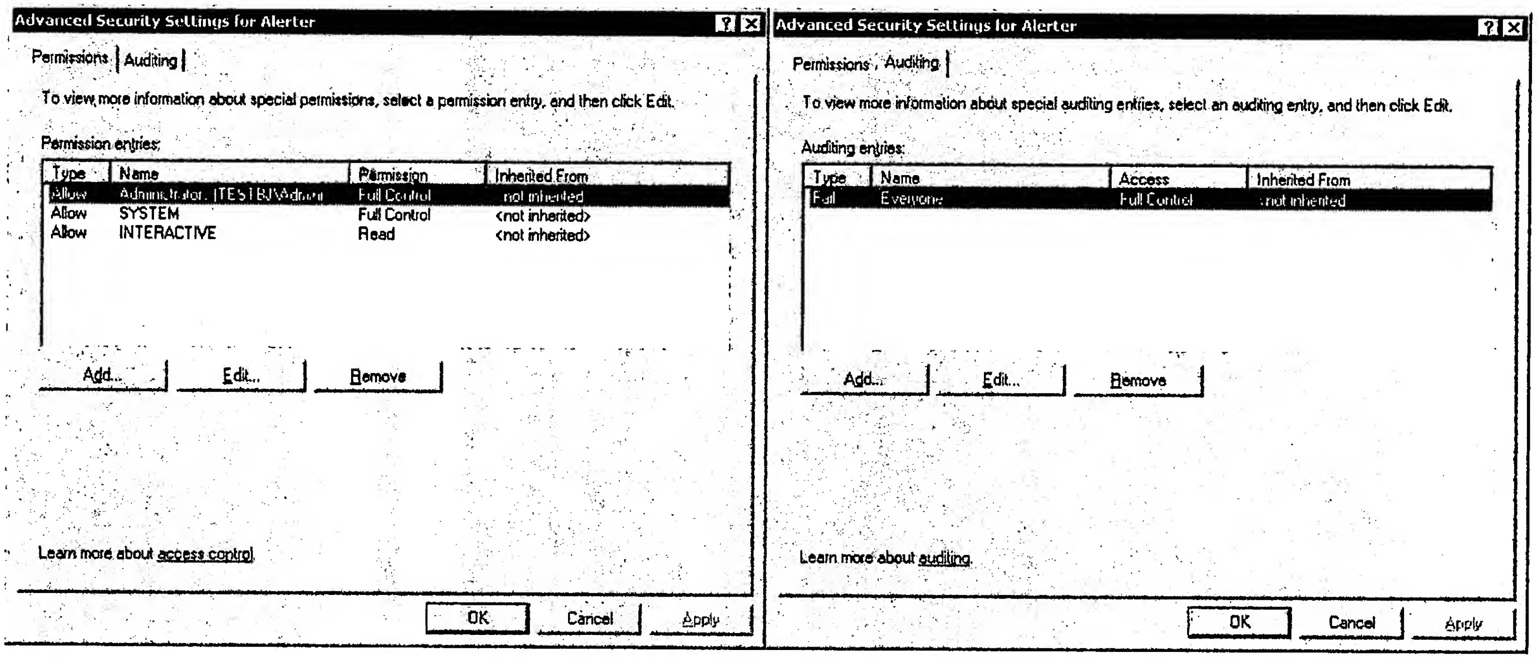
Select file extension:

Application precedence:

Categories for bjdomain.nttest.microsoft.com

Software Installation	
General	
Policy	**Security Setting**
Add data here	10 minutes
Advanced	
Policy	**Security Setting**
Add data here	COMCFG; DFS$
File Extensions	
Policy	**Security Setting**
Add data here	COMCFG; DFS$
Categories	
Policy	**Security Setting**
Add data here	Enabled

FIG. 11



Advanced Security Settings for Alerter
? ×
Permissions
Auditing

To view more information about special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From
Allow	Administrator (TESTBJ\Admini	Full Control	not inherited
Allow	SYSTEM	Full Control	<not inherited>
Allow	INTERACTIVE	Read	<not inherited>

Learn more about access control.

OK
Cancel
Apply
Advanced Security Settings for Alerter
? ×
Permissions
Auditing

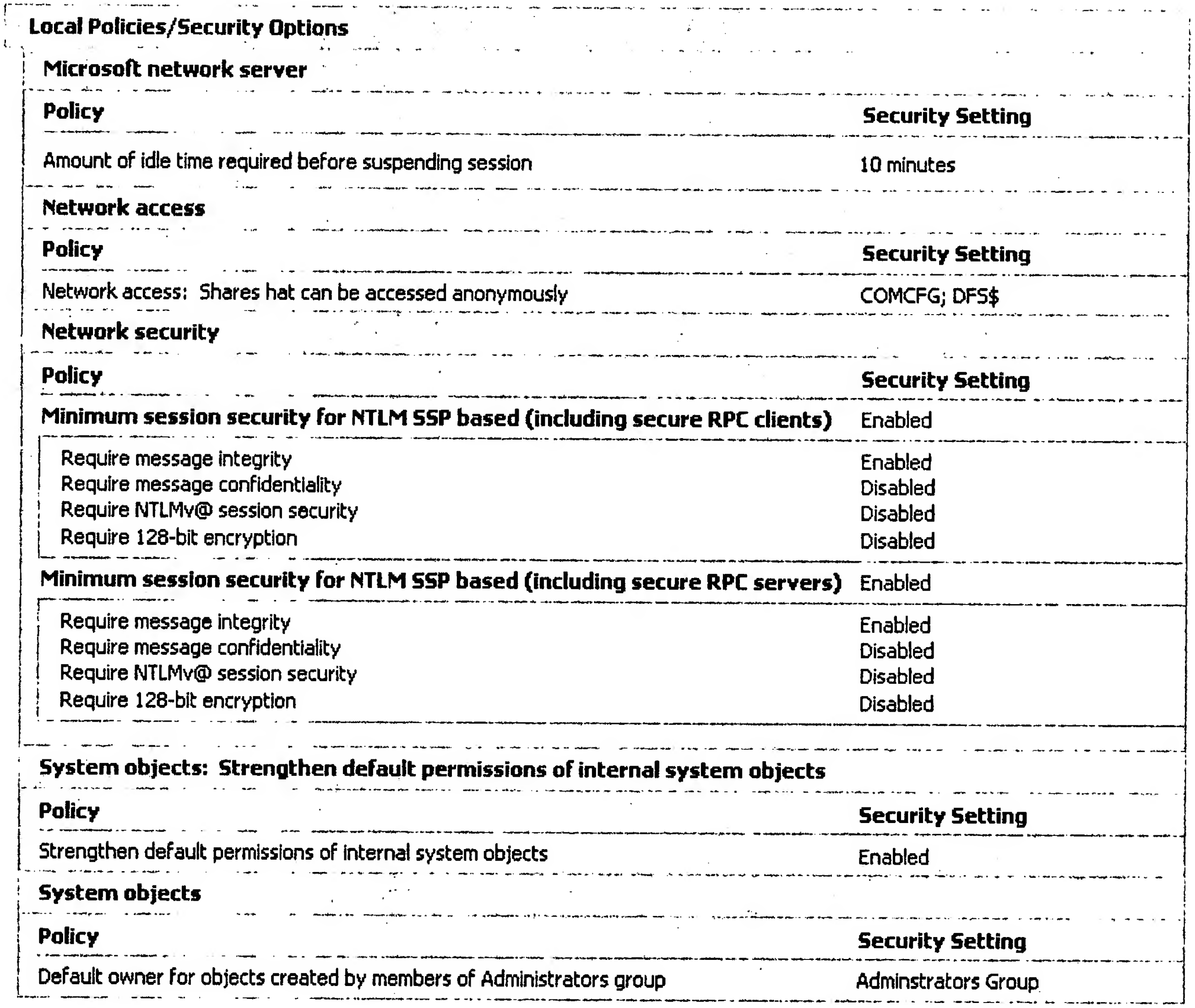
To view more information about special auditing entries, select an auditing entry, and then click Edit.

Auditing entries:

Type	Name	Access	Inherited From
Fail	Everyone	Full Control	not inherited

Learn more about auditing.

FIG. 13
Prior Art



Local Policies/Security Options

Microsoft network server

Policy	**Security Setting**
Amount of idle time required before suspending session	10 minutes

Network access

Policy	**Security Setting**
Network access: Shares hat can be accessed anonymously	COMCFG; DFS$

Network security

Policy	**Security Setting**
Minimum session security for NTLM SSP based (including secure RPC clients)	Enabled
Require message integrity	Enabled
Require message confidentiality	Disabled
Require NTLMv@ session security	Disabled
Require 128-bit encryption	Disabled
Minimum session security for NTLM SSP based (including secure RPC servers)	Enabled
Require message integrity	Enabled
Require message confidentiality	Disabled
Require NTLMv@ session security	Disabled
Require 128-bit encryption	Disabled

System objects: Strengthen default permissions of internal system objects

Policy	**Security Setting**
Strengthen default permissions of internal system objects	Enabled

System objects

Policy	**Security Setting**
Default owner for objects created by members of Administrators group	Adminstrators Group

FIG. 14

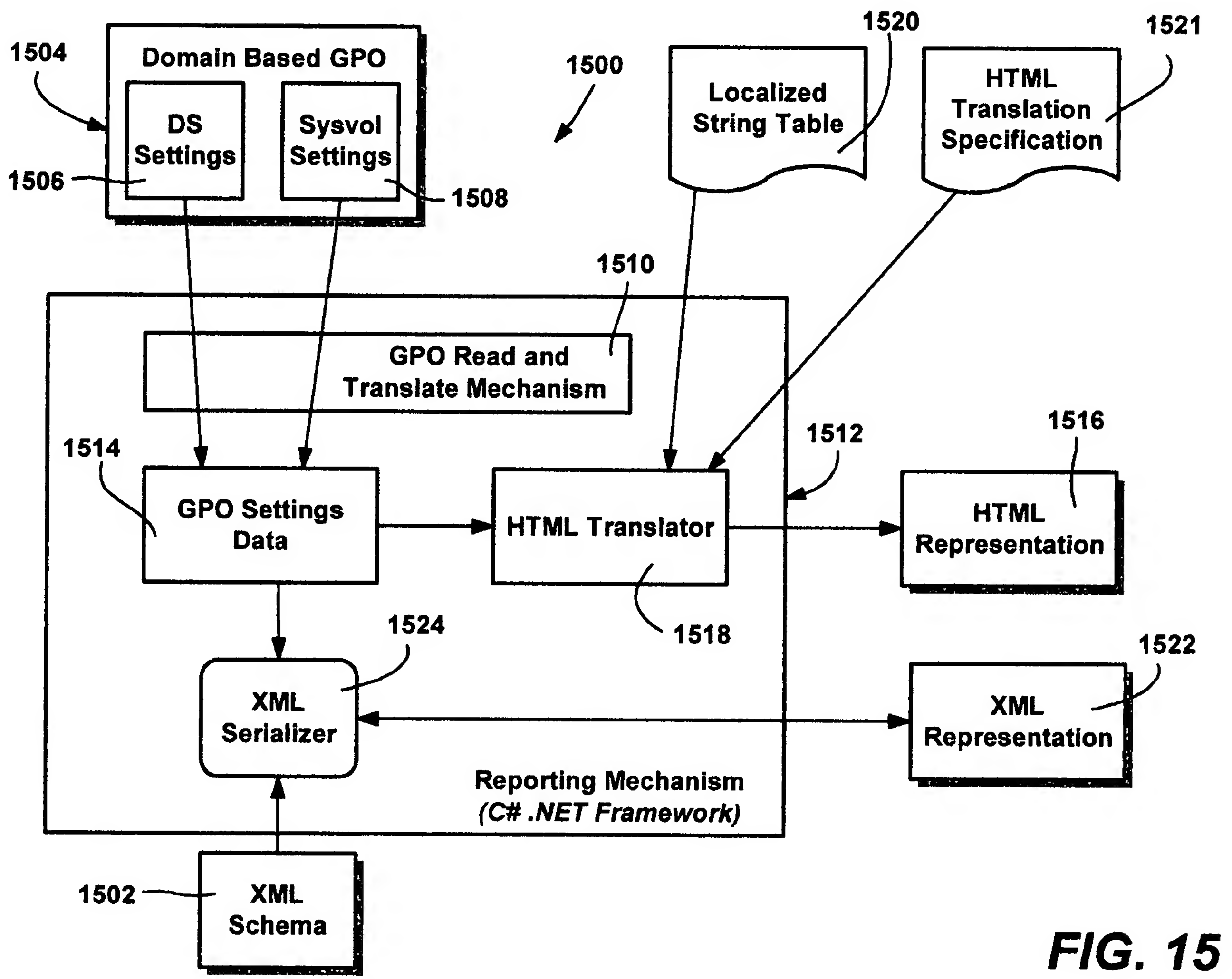

1504
Domain Based GPO
DS Settings
1506
Sysvol Settings
1508
1500
Localized String Table
1520
HTML Translation Specification
1521
1510
GPO Read and Translate Mechanism
1514
GPO Settings Data
HTML Translator
1518
1512
HTML Representation
1516
1524
XML Serializer
XML Representation
1522
Reporting Mechanism
(C# .NET Framework)
1502
XML Schema

FIG. 15

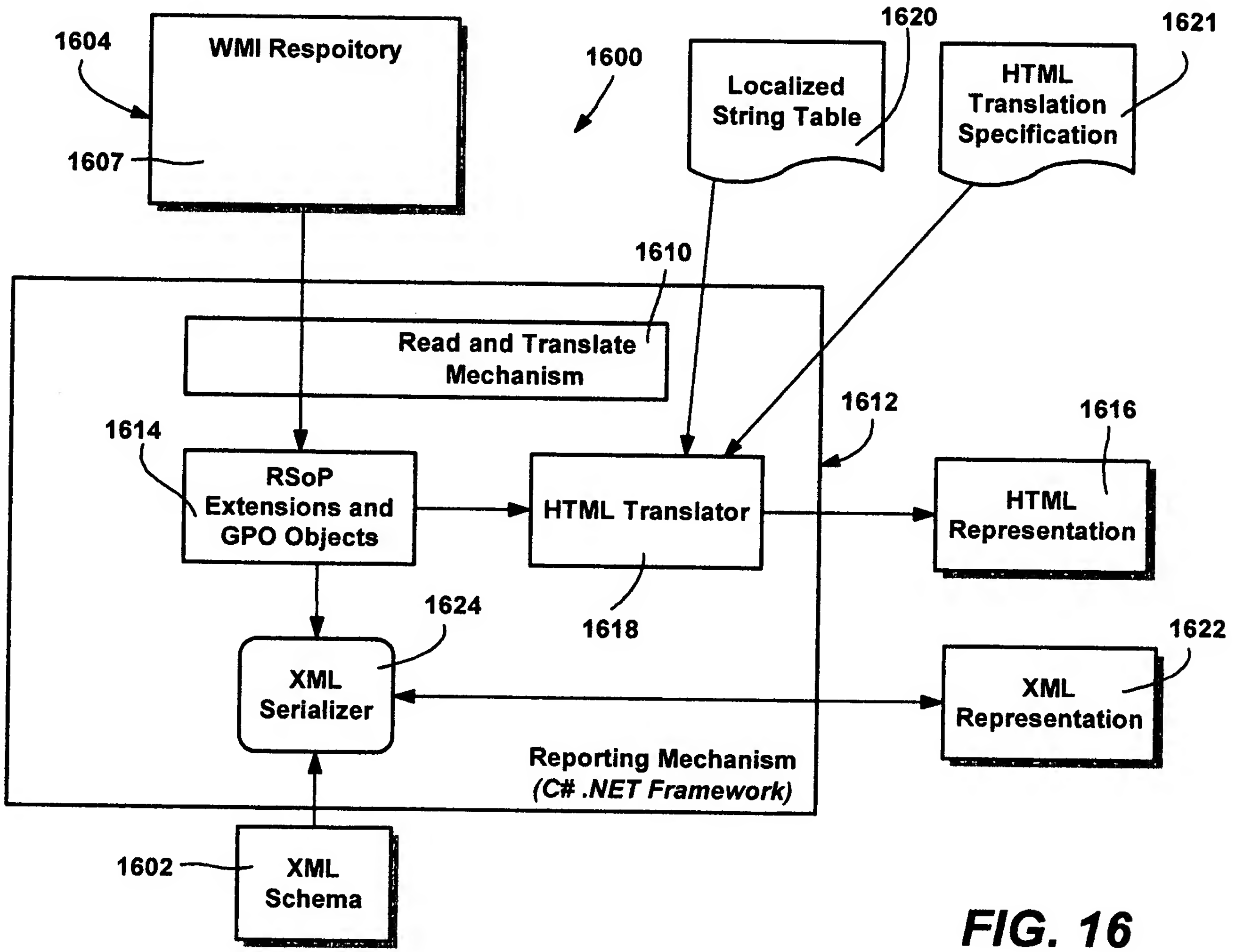
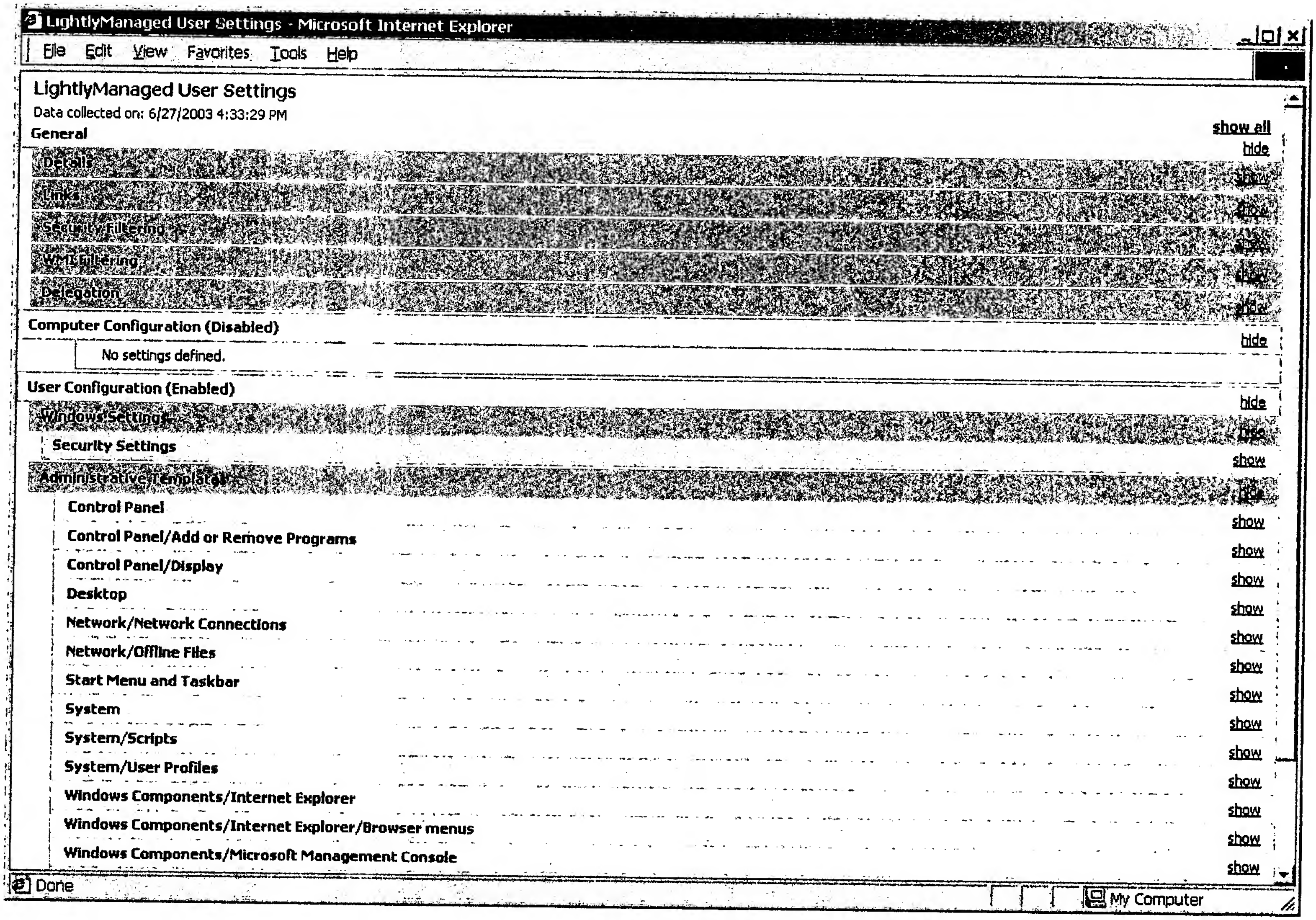

1604
WMI Respoitory
1607
1600
Localized
String Table
1620
HTML
Translation
Specification
1621
1610
Read and Translate
Mechanism
1614
RSoP
Extensions and
GPO Objects
HTML Translator
1618
1612
1616
HTML
Representation
1624
XML
Serializer
1622
XML
Representation
Reporting Mechanism
(C# .NET Framework)
1602
XML
Schema

FIG. 16

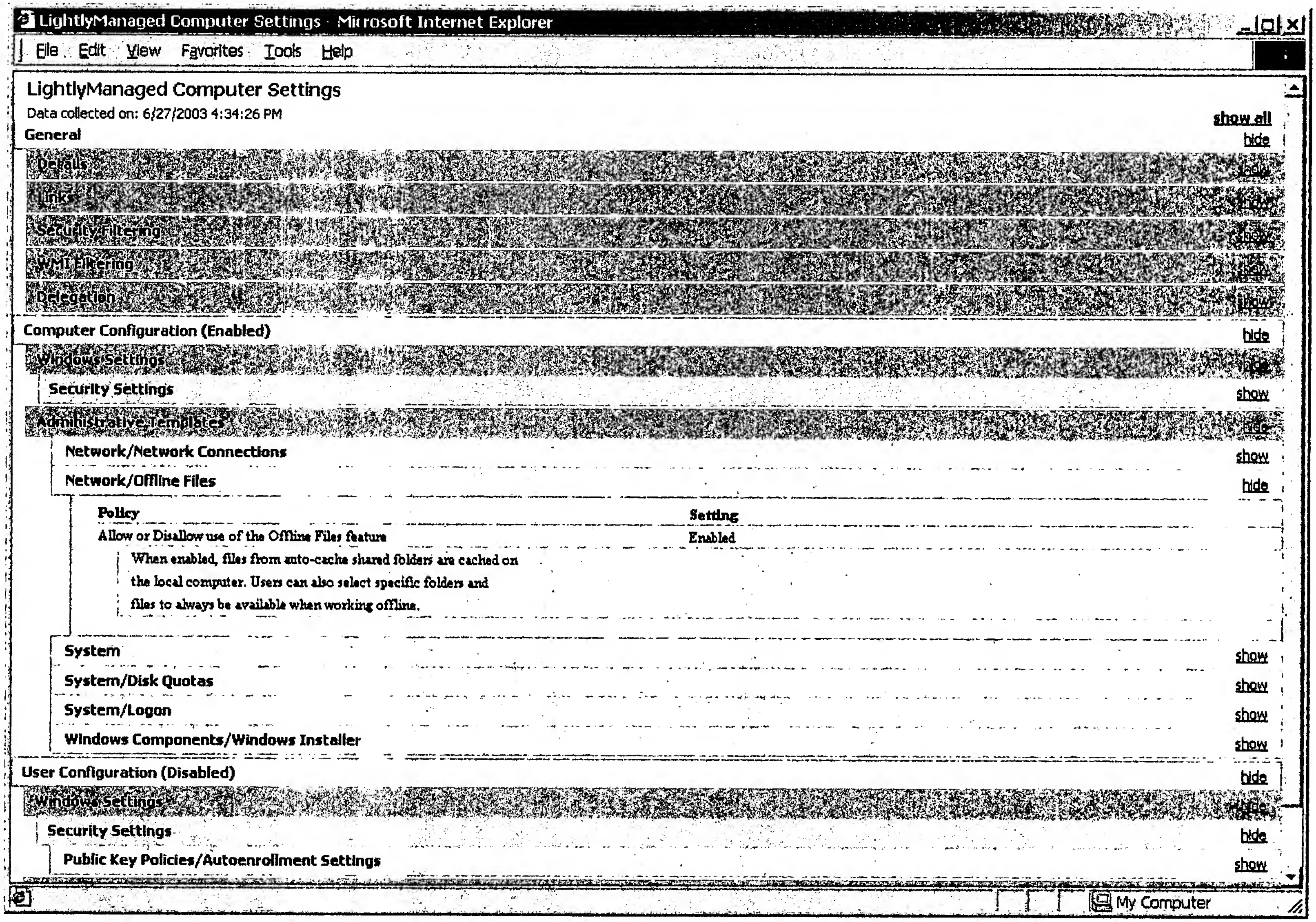

LightlyManaged User Settings - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Done
My Computer

LightlyManaged User Settings

Data collected on: 6/27/2003 4:33:29 PM

General	show all
	hide
Details	show
Links	show
Security Filtering	show
WMI Filtering	show
Delegation	show
Computer Configuration (Disabled)	hide
No settings defined.	
User Configuration (Enabled)	hide
Windows Settings	hide
Security Settings	show
Administrative Templates	hide
Control Panel	show
Control Panel/Add or Remove Programs	show
Control Panel/Display	show
Desktop	show
Network/Network Connections	show
Network/Offline Files	show
Start Menu and Taskbar	show
System	show
System/Scripts	show
System/User Profiles	show
Windows Components/Internet Explorer	show
Windows Components/Internet Explorer/Browser menus	show
Windows Components/Microsoft Management Console	show

FIG. 17


LightlyManaged Computer Settings - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
My Computer

LightlyManaged Computer Settings

Data collected on: 6/27/2003 4:34:26 PM

show all

General hide

Details show

Links show

Security Filtering show

WMI Filtering show

Delegation show

Computer Configuration (Enabled) hide

Windows Settings hide

Security Settings show

Administrative Templates hide

Network/Network Connections show

Network/Offline Files hide

Policy	Setting
Allow or Disallow use of the Offline Files feature	Enabled

When enabled, files from auto-cache shared folders are cached on the local computer. Users can also select specific folders and files to always be available when working offline.

System show

System/Disk Quotas show

System/Logon show

Windows Components/Windows Installer show

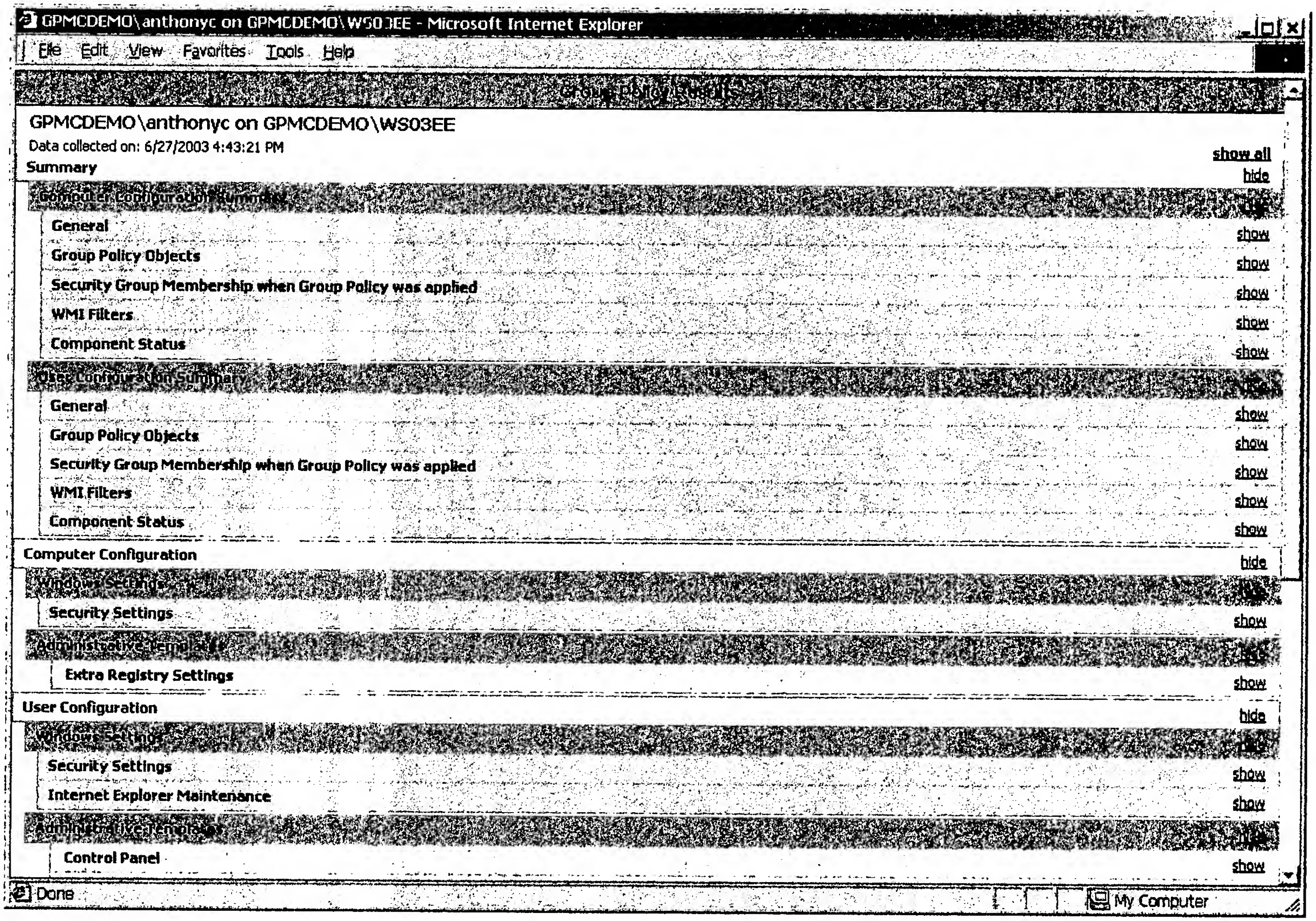
User Configuration (Disabled) hide

Windows Settings hide

Security Settings hide

Public Key Policies/Autoenrollment Settings show

FIG. 18



GPMCDEMO\anthonyc on GPMCDEMO\WS03EE - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Done
My Computer

Group Policy Results

GPMCDEMO\anthonyc on GPMCDEMO\WS03EE
Data collected on: 6/27/2003 4:43:21 PM

show all

Summary hide

Computer Configuration Summary hide

General show
Group Policy Objects show
Security Group Membership when Group Policy was applied show
WMI Filters show
Component Status show

User Configuration Summary hide

General show
Group Policy Objects show
Security Group Membership when Group Policy was applied show
WMI Filters show
Component Status show

Computer Configuration hide

Windows Settings hide

Security Settings show

Administrative Templates hide

Extra Registry Settings show

User Configuration hide

Windows Settings hide

Security Settings show
Internet Explorer Maintenance show

Administrative Templates hide

Control Panel show

FIG. 19